In order to competently ensure that software and configuration vulnerabilities in FSA's systems and major applications do not impact mission and business critical operations, to comply with FISMA, the Security & Privacy Group recommends,

Between **December 2003 and March 2004**, BearingPoint researched and prepared documents specifically about patch management. A couple of meetings with, and presentations from, vendors were made. Patch Management was defined and researched in a document entitled Introduction to Patch Management.

Between **March 29 and April 14**, a presentation entitled Security Patch Management – Preparing the Case for Automation was created to identify the following:

1. Business Reasons for Implementing Automated Security Patch Management at FSA
2. The Current Climate of Rapid Vulnerability/Patch Release
3. Pertinent Regulatory Requirements and Recommendations
4. Methods of Security Patch Management

The presentation also summarized the advantages of automation and centralization; it's functional and reporting capabilities, and recommended strategy for moving forward.

March 29-July 31
The Security and Privacy Group continuously communicates and coordinates with SSO, contractor representatives, and other key personnel, to evaluate needs and strategies for program cooperation.

April 15-
Research of commercial solutions to accommodate the FSA environment was stepped up to include demonstrations from three vendors and research and teleconferences with several more.

As a result of the research, it was determined that the scope of security patch management would need to allow for "management" of more than simply patches to be effective. Though patch management is critical, software and device misconfigurations, and other vulnerabilities exist. These could be managed by expanding on the same technology that is a key component of patch management solutions, i.e., the real time discovery and detection functionality.

- ❑ Patchlink – Originally previewed in early December by the Security and Privacy Group. PatchLink's federal representative was invited in April to discuss the product's capabilities and relevance in the FSA environment. PatchLink enabled access to a live running test environment (via web browser) at their headquarters. Functionality for version 5 was reviewed and evaluated:
    - o Discovery of assets, detection of vulnerabilities, and aggregation of the data at a PatchLink Server, are accomplished via agents placed on individual machines. The solution does not accommodate the use of the agent to perform discovery and detection, and remediation of settings and configurations. As

Copyright 2004, BearingPoint, Inc.

the evaluation of solutions, in general has evolved, it has become apparent that this functionality is critical in the long run.

- A heavy emphasis is placed on the solution's ability to effectively maintain a central database of pre-tested, multiplatform, patches and accompanying remediation advice. PatchLink is a very efficient and effective tool for centrally applying patches and tracking their automated deployment. The outsourced nature of FSA environment will not immediately lend to centralized deployment of patches. The PatchLink solution would have to be imposed on all relevant contractors for it to be cost-beneficial. PatchLink has acknowledged that central control of more than one PatchLink server is in the works. Even so, PatchLink's focus is deployment.

- BigFix/SecureInfo – SecureInfo was responsible for the FedCirc PADC program (cancelled to new customers circa 4/1/04), as a reseller of the BigFix product. SecureInfo had as its goal, the integration of a comprehensive vulnerability database with BigFix, allowing agencies to seamlessly discover vulnerabilities requiring patches, settings changes, and/or other configuration measures. To date, SecureInfo has not accomplished this integration. They have tentatively scheduled to allow FSA to interact with a live demo of this integration on June 1st. Nevertheless, the BigFix product (via SecureInfo and PADC)

    - Also agent-based, BigFix uses an additional component, that of a relay server, to cut down on network traffic, and create more flexibility and efficiency in architecture and organizational requirements. The agent has an API that allows it to perform tasks in addition to traditional "patch management".

    - BigFix has a very intuitive user interface that is windows rather than web based. It's discovery and detection capability combined with associated highly manipulative views, make it a valuable inventory tool.

    - BigFix maintains a database of multiplatform vulnerabilities and remediation advice but not the patches themselves. Patches are acquired via a validated link to the ISV supplied url or ftp site. A patch is downloaded to the BigFix Enterprise Server residing at the customer (FSA) site and mass deployment can be accomplished.

- Symantec iCommand and Enterprise Security Manager (ESM) – Symantec has two pieces to the puzzle that are yet to be fully integrated. ICommand uses an OEM version of HFNetChk Pro, a patch management solution that utilizes scanning technology. ESM is an agent-based product that tries to be all things to all things security related and it is difficult to understand the value relative to FSA's patch and vulnerability management needs. Nevertheless, Symantec is quite sensitive to the type of solution that FSA needs and admits to falling short at this point in time.

Copyright 2004, BearingPoint, Inc.

- Marimba – The company was recently (4/1/04) acquired by BMC Software, mfrs. of help desk king, Remedy. The product has not been evaluated yet. It is in the works. High interest in the integrated Marimba/Remedy Action Response products.

- Scan-based tools – Scanners and patch management products that use scanning to discover and detect, can do discovery and detection very well but must be run periodically at off-peak network hours because of their encumbrance on bandwidth. However, if scanning technology was paired with scripts that could automatically report any changes a quasi-real time detection environment could be accomplished. Eeye digital's newly announced Beta version of it's Retina v5.0 incorporating patch management is worthy of evaluating.

- Other – SecurityProfiling, Inc., Patch Advisors – Young, innovative companies with the right idea but not enough history yet.

May 4 – May 14
The Security and Privacy Group mapped out a workflow for Security Vulnerability and Patch Management. The workflow is based on real-time discovery of weaknesses, classifying them, and taking action. It includes as critical to its success, a means of accountability and enforcement. Roles and responsibilities are defined and a product recommendation is made for the proof of concept. **The proof of concept is necessary to define and refine the accountability piece of this solution.**

May 17 – June 1
Logistics for deployment of proof of concept are prepared and defined. Personnel required to deploy are identified. Senior management approval is required.

June 1-July 15
Proof of Concept Implementation (See Attached Document – FSA Vulnerability/Patch Management)

June 1 – July 30
Gather Requirements, Get Buy In, Line Up Resources for Pilot and Phase In Enterprise Tool(s).

July 15-July 30
Select Product(s)

August 1-August 15
Run Pilot

August 15-September 1
Prepare and Release Procurement

September 1 – September 30
Purchase and Deploy

Copyright 2004, BearingPoint, Inc.

Vulnerability Assessment & Remediation Integration Project

Task	Dec 03-Feb 04						Mar 04				Apr 04				May 04				Jun 04				Jul 04				Aug 04				Sep 04			
Patch Management Research Briefing	▨	▨	▨	▨	▨	▨	▨																											
Case For Automation Briefing										▨	▨	▨																						
Communicate & Coordinate w/ SSO's and Data Center Management										▨	▨	▨	▨	▨	▨	▨	▨	▨	▨															
Research Commercial Tools & Solutions													▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨								
Map Out Workflow, Define Roles & Responsibilities															▨	▨																		
Prepare and Finalize Logistics for Deployment of Proof of Concept																	▨	▨																
Deploy Proof of Concept																			▨	▨														
Gather Requirements, Perform Targeted ID and Remediation and Chart Progress																			▨	▨	▨	▨	▨	▨										
Assess Response. Enable contractor use of tool for better response if needed.																					▨	▨	▨	▨										
Evaluate contractor use of tool																					▨	▨	▨	▨										
Revise Workflow and Accountability Roles & Responsibilities as Needed																					▨	▨	▨	▨										
Select Product(s)/Tools for Pilot																									▨	▨								
Determine Final Costs Estimate																									▨	▨	▨							
Purchase Products/Tools/Services																											▨	▨	▨	▨				
Deploy Phase II – Full VDC																															▨	▨		
Deploy Phase III – Extend To Rockville																																▨	▨	
Deploy Phase IV – Extend to other																																	▨	▨

Copyright 2004, BearingPoint, Inc.

Vulnerability Assessment & Remediation Integration Project

Proof of Concept Requirements

Product	Agent Based?	MultiPlatform?	Deep Visibility To Inspect all configuration Information? Can accept multiple sources of patch and remediation advice.	Agent open (API) to allow for performance of tasks aside from patch deployment?	Intuitive User Interface. Multiple views and sorting and grouping for monitoring, reporting, and action	Encryption and digital signature validation	Can be integrated into other enterprise reporting systems?	Can allow other enterprise detection and reporting systems to integrate?	
PatchLink	Yes	Yes	No	No	Acceptable	Yes	Yes	No	
BigFix	Yes	Yes	Yes	Yes	Superior	Yes	Yes	Yes	
Symantec	No	Yes/No	Yes		Superior	Yes	Depends	No	
Other Scan Based					Acceptable	??	Depends	No	

Pilot and potential purchase Advanced requirements

Product	Workflow	Automated Accountability Techniques	Messaging	Seamless integration for Unified Console	Automated Reporting	Future Functionality	Scalability	Cost
PatchLink								
BigFix								
Symantec								
Marimba/Remedy								
Other								

Copyright 2004, BearingPoint, Inc.